Notice of Allowability	**Application No.** 09/539,928	**Applicant(s)** WARRIER ET AL.	
	Examiner Ellen C. Tran	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *1 January 2006*.

2. ☒ The allowed claim(s) is/are *17-23 and 29-46*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) ☐ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

   1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.

   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Examiner's Amendment and Reasons for Allowance

1. In response to amendment filed on 17 January 2006.

2. An examiner's amendment to the record is attached. Please enter entire claim set. The attached amendment adds details to independent claims 17 and 21. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Allowable Subject Matter

3. The following is an examiner's statement of reasons for allowance: Claims 17-23 and 29-46 are allowed, in view of amendment to claims as well as arguments beginning on page 12, "Freund fails to describe or otherwise suggest delivering security policies from a server to a remote server during initialization of a VPN". The claimed invention also teaches implementing security policies based on the running state or priority of an application, this is not taught in any of the other prior art of references in combination with delivering VPN connection and delivering policies remotely directly to a computer system.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance".

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 2:30 pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen. Tran
Patent Examiner
Technology Center 2134
31 March 2006

ECT

EXAMINER'S AMENDMENT:

This listing of claims replaces all prior versions, and listings, of claims in the application:

1-16 (Canceled).

17. (Currently Amended) A network system, comprising:

first and second devices, wherein

the first device is adapted to:

deliver a set of policies to the second device during initialization of a virtual private network between the first and second devices; and

the second device is remote from the first device and adapted to:

run an application;

use both said policies and a priority assigned to the application to detect data packets from unauthorized activities; and

reject data packets from the unauthorized activities.

18. (Original) The system of claim 17 further comprising a network stack.

19. (Original) The system of claim 18, wherein the network stack comprises:

a policy engine connected to the first device;

a policy store connected to the policy engine;

a socket interceptor connected to the policy engine; and

a packet guard connected to the policy engine.

20. (Original) The system of claim 17, the first device further comprising instructions to monitor the system for the intervening processes.

21. (Currently Amended) A network stack, comprising:

a policy engine;

a policy store adapted to interact with the policy engine and store a set of policies from the policy engine;

a socket interceptor coupled to the policy engine;

a packet guard coupled to the policy engine;

a configurable management process adapted to reconfigure the network stack and having instructions to:

receive policies in the policy engine from the policy server during a virtual private network session with a remote device;

use the socket interceptor to detect and reject data packets from unauthorized users and applications and provide the packet guard with context information about the unauthorized users and applications including at least information ~~a priority~~ about a running state of the application;

use the packet guard to filter unauthorized activities received from the network interface;

use the packet guard to filter the data packets from unauthorized users and applications based on the context information received by the socket interceptor; and

use the packet guard to filter data packets based on the policies.

22. (Original) The network stack of claim 21 further comprising a packet translator adapted to interact with the socket interceptor and the packet guard.

23. (Original) The network stack of claim 21 further comprising an interface to a network adapted to connect the

network stack to the network, wherein the network has a policy server.

24-28. (Canceled)

29. (Previously Presented) A system as in claim 17, wherein said second device uses said policies to determine if an application is running and allows certain kinds of network packets, associated with said network application, to pass only when said application is running and to be blocked when said application is not running.

30. (Previously Presented) A method comprising:

establishing a virtual private network (VPN) session between a primary computing system and a remote computing system, wherein the primary computing system includes a security policy engine, and wherein the remote computing system includes a network stack;

transmitting information indicative of security parameters from the primary computing system to the remote computing system using the security policy engine during initialization of the VPN;

configuring the network stack based on the information indicative of security parameters;

subsequently running a particular application program on the remote computing system;

selecting information indicative of updated security parameters based on a priority of the particular application program; and

dynamically reconfiguring the network stack based on the information indicative of the updated security parameters.

31. (Previously Presented) The method of claim 30, wherein the primary computing system is a corporate local area network (LAN).

32. (Previously Presented) The method of claim 30, wherein the remote primary computing system is a remote home network.

33. (Currently Amended) The method of claim 30, wherein the particular application program is a data ~~word~~ processing program, and wherein, when a running state of the data ~~word~~ processing program indicates that the data ~~word~~ processing program is not running, the information indicative of security

parameters causes the remote computing system to block ~~word processing~~ packets received at the remote computing system.

34. (Currently Amended) The method of claim 30, wherein the particular application program is a data word processing program, and wherein, when a running state of the data ~~word~~ processing program indicates that the data ~~word~~ processing program is running, the information indicative of updated security parameters causes the remote computing system to not block ~~word processing~~ packets received at the remote computing system.

35. (Previously Presented) A method comprising:

establishing a secure virtual private network connection between a server and a remote system;

delivering security policies from the server to the remote system during initialization of the secure private network connection; and

regulating access to nodes accessible via the server by the remote system based on the security policies and a priority associated with at least one application program running on the remote system.

36. (Previously Presented) The method of claim 35 wherein regulating access comprises providing filters that are adapted to reject unauthorized data packets based on rejection criteria that are conditioned on the security policies and the priority of the at least one application program.

37. (Previously Presented) The method of claim 35 wherein regulating access comprises:

providing a session layer adapted to reject unauthorized data packets based on context information; and

providing filters adapted to reject unauthorized data packets based on rejection criteria from at least one of the context information and the policies.

38. (Previously Presented) The method of claim 35 further comprising updating the set of policies.

39. (Previously Presented) The method as in claim 35, wherein the remote system includes a network stack, and wherein the regulating access comprises reconfiguring the network stack to control filtering of network packets, based on the policies and the priority of the application.

40. (Previously Presented) The method as in claim 35, wherein the policies include information about authorized kinds of information when certain applications are running, and regulating access comprises determining if a specified application is running, allowing a specified kind of network packet to pass only when the specified application is running, and blocking the specified kind of network packet from passing when the specified application is not running.

41. (Previously Presented) The method as in claim 40, wherein the specified application is a word processing program, and the kind of network packet is word processing data.

42. (Previously Presented) An article comprising a computer-readable medium which stores computer-executable instructions, the instructions causing a computer to:

establish a secure virtual private network connection between a server and a remote system;

deliver security policies from the server to the remote system during initialization of the secure private network connection; and

regulate access to nodes accessible via the server by the remote system based on the security policies and a priority associated with at least one application program running on the remote system.

43. (Previously Presented) The article of claim 42 wherein regulating access comprises providing filters that are adapted to reject unauthorized data packets based on rejection criteria that are conditioned on the security policies and the priority of the at least one application program.

44. (Previously Presented) The article of claim 42 wherein regulating access comprises:

providing a session layer adapted to reject unauthorized data packets based on context information; and

providing filters adapted to reject unauthorized data packets based on rejection criteria from at least one of the context information and the policies.

45. (Previously Presented) The article of claim 42 further comprising updating the set of policies.

46. (Previously Presented) The article as in claim 42, wherein the policies include information about authorized kinds of information when certain applications are running, and

regulating access comprises determining if a specified application is running, and allowing a specified kind of network packet to pass only when the specified application is running, based on the policies, and, blocking the specified kind of network packet from passing, when the specified application is not running, based on the policies.